

خلاصه اجرایی

هایپرلیکوئید به محض شناسایی یک آدرس به عنوان «پرخطر»، دسترسی آن را مسدود می‌کند. این هشدار معمولاً به صورت یک نوار قرمز در پنل معاملاتی نمایش داده شده و دلیل مسدودسازی را به کاربر اطلاع می‌دهد. آدرس‌های پرخطر معمولاً شامل مواردی مانند تعامل با آدرس‌های تحریمی یا دارایی سرقت شده، استفاده از میکسرهای رمزارز، یا رفتاری هستند که الگوریتم‌های تجزیه و تحلیل بلاک چین آن را مشکوک ارزیابی می‌کنند. برای رفع این مشکل، نخست باید اسکرین‌شات پیام هشدار و اطلاعات حساب خود را ثبت کرده و سپس یک تیکت پشتیبانی رسمی به آدرس support@hyperliquid.zendesk.com ارسال کنید [L142-L149+43] [53+L240-L249]. در تیکت، آدرس عمومی والت، متن هشدار و اسکرین‌شات آن، تاریخ و دارایی‌های قابل برداشت خود را به وضوح بیان کنید. در کنار این اقدامات، استفاده از روش‌های موقتی مانند برداشت از طریق API یا انتقال دارایی به یک آدرس جایگزین (مانند رید کردن از طریق **deBridge** یا سایر پل‌های میان‌رشته‌ای) می‌تواند به شما امکان خروج از موقعیت را بدهد [L149-L157+19] [18+L243-L252]. در هر مرحله، از اشتراک‌گذاری کلید خصوصی خودداری کنید (پشتیبانی‌های رسمی هرگز کلید خصوصی درخواست نمی‌کنند [L67-L71+43])، و در صورت توقف روند پاسخگویی، ممکن است لازم شود بعد از چند هفته اقدام به پیگیری شکایات رسمی یا مشورت حقوقی کنید [L117-L124+71] [71+L124-L132]. در جدول زیر مقایسه‌ای از چند ابزار مشهور اسکرینینگ و نمونه پرچم‌های متداول آن‌ها آمده است.

ابزار/سرویس	ویژگی‌ها/نکته کلیدی	نمونه‌ی پرچم‌های متداول
Chainalysis	تحلیل عمیق بلاک چین؛ استفاده ۹ از ۱۰ صرافی برتر [L262-L270+36]	تحریم‌ها (OFAC)، آدرس‌های هک شده، دارکنت، کلاهبرداری
Elliptic	رصد چندزنجیره‌ای (تحلیل ریسک بین‌زنجیره‌ای) [L52-L60+31]	تحریم‌ها، پولشویی، شبکه‌های مخفی معامله
TRM Labs	مانیتورینگ بلادرنگ تراکنش‌ها (قوی در سولانا/ترون) [L53-L60+31]	پولشویی، تبادل پایدارکوین با ریسک بالا، تراکنش‌های پیچیده
Crystal	پوشش گسترده (بیش از ۳۳۵ زنجیره) [L55+31-L60]	تراکنش‌های سرقت شده، شستن (wash trading)، فعالیت‌های غیرقانونی
Scorechain	تمرکز بر بازار اروپا، ارائه API اسکن رایگان تحریم [L59-L60+31]	اسکن فهرست تحریم‌ها، ردیابی دامنه کیف‌ها
Blockaid (Hyperliquid)	حل و فصل بلادرنگ ریسک برای هایپرلیکوئید [L11-L15+74]	تحریم‌ها، دارایی‌های سرقت شده، اسکم/کلاهبرداری، تعامل با میکسر [L100-L104+73]

دلایل احتمالی بلاک شدن آدرس

سیستم‌های غربالگری بلاک چین آدرس‌ها را بر اساس شاخص‌های پولشویی و تروریسم مالی، فهرست‌های تحریم، و الگوهای تراکنشی غیرعادی بررسی می‌کنند [L49-L58+7] [51+L80-L87]. برای مثال، یک آدرس ممکن است به خاطر تعامل با یک کیف پول تحریمی یا سابقه منتقل کردن دارایی از/به میکسر رمزارز (مثل تامیدور توکن) پرچم‌گذاری شود [L100-L104+73] [51+L80-L87]. علاوه بر این، الگوریتم‌ها ممکن است فعالیت‌هایی مانند حضور چندباره در ICO/ایردراپ‌های مشکوک یا استفاده از قراردادهای ناشناس را نیز پرخطر تلقی کنند [L112-L115+14] [L80-L87+51]. برخی کاربران متوجه شده‌اند که استفاده از VPN یا آی‌پی از کشورهای محدود ممکن است واکنش بگیرد (اگرچه این مورد به طور رسمی تأیید نشده است). همچنین اگر یک آدرس در دسته‌های شبکه‌ای با آدرس‌های مشکوک باشد (مثلاً از طریق پیوندهای تراکنش غیرمستقیم)، غربالگری آن را جدی می‌گیرد [L80-L87+51]. در کل، هرگونه ارتباط زنجیره‌ای با نهادهای نایمن/تحریمی، استفاده از میکسر، تعامل با قراردادهای «اسکم» یا فعالیت‌های غیرمعمول، می‌تواند منجر به پرچم‌گذاری شود [L80-L87+51] [14+L112-L115].

【embed_image+72】 نمونه‌ای از پیغام هشدار «آدرس پرخطر» در پنل معاملاتی *Hyperliquid*. این خطای نوار قرمز رنگ به کاربر می‌گوید آدرس او توسط ابزار غربالگری سوم شخص «پرخطر» تشخیص داده شده است (در این مثال می‌توانید متن کامل هشدار را ببینید) 【L80-L87+51】
【L112-L115+14】.

ابزارهای غربالگری رایج و استفاده در Hyperliquid

برای مطابقت با مقررات AML/KYC، بسیاری از پلتفرم‌های رمزارز از شرکت‌های تحلیل بلاک‌چین شناخته‌شده استفاده می‌کنند. **Chainalysis** به‌عنوان یکی از پیشروها شناخته می‌شود (۹ از ۱۰ صرافی بزرگ دنیا از آن استفاده می‌کنند 【L262-L270+36】). سایرین مانند **TRM**، **Elliptic**، **Crystal Intelligence** و **Scorechain** نیز در بازار رایج هستند 【L44-L52+31】. این ابزارها هر کدام قابلیت‌های ویژه‌ای دارند؛ برای نمونه Chainalysis پوشش زنجیره‌ای وسیعی دارد، Elliptic بر تحلیل بین‌زنجیره‌ای متمرکز است، TRM روی بررسی لحظه‌ای تراکنش و VASP‌ها تمرکز می‌کند، Crystal بیشترین تعداد زنجیره پشتیبانی را دارد، و Scorechain به‌ویژه در بازار اروپا طرفدار است 【L44-L52+31】.

هایپرلیکوئید به‌طور مشخص با **Blockaid** همکاری دارد. بانک مرکزی هایپرلیکوئید در اکتبر ۲۰۲۵ اعلام کرد که Blockaid از زنجیره HyperEVM پشتیبانی کامل می‌کند 【L11-L15+74】. Blockaid در گزارشات خود اشاره می‌کند که تراکنش‌ها را در زمان واقعی بررسی می‌کند و مواردی مانند تحریم‌ها، دارایی‌های مسروقه، کلاهبرداری و میکسرها را در زمره معیارهای ریسک قرار می‌دهد 【L100-L104+73】 【L74+L11-L15】. به‌طور خلاصه، ابزارهای غربالگری خارجی مجموعه‌ای از فهرست‌های تحریم و شاخص‌های رفتاری را در نظر می‌گیرند و Hyperliquid نیز با بهره‌گیری از خدمات Blockaid این کار را انجام می‌دهد 【L11-L15+74】 【L73+L100-L104】.

【embed_image+75】 نمایی از داشبورد ابزار تحلیلی *Blockaid*: این تصویر نمونه‌ای از تحلیل بلاک‌چین ریسک‌های یک آدرس را نشان می‌دهد (برای هایپرلیکوئید). در این نما، دسته‌های مختلفی مثل «دارایی‌های مسروقه» (*Stolen Funds*)، «استفاده از میکسر رمزارز» (*Crypto Mixer*) و «کلاهبرداری» (*Scam/Fraud*) دیده می‌شود که هر یک به صورت درصدی از ریسک کل اندازه‌گیری شده‌اند 【L100-L104+73】.

مراحل رفع مشکل و ارسال تیکت پشتیبانی

1. ثبت اطلاعات حساب: پیش از هر چیز، از پیام هشدار اسکرین‌شات بگیرید و وضعیت حساب (موجودی‌ها، موقعیت‌های باز، تراکنش‌های اخیر) را یادداشت کنید 【L240-L249+53】 【51+L93-L100】. این اطلاعات شامل آدرس عمومی کیف پول و تاریخچه تراکنش‌های مرتبط با سیرده/برداشت می‌شود. (از اشتراک‌گذاری اطلاعات خصوصی یا کلید خصوصی خودداری کنید 【L67-L71+43】).
2. ارسال تیکت پشتیبانی: به وبسایت پشتیبانی Hyperliquid مراجعه کرده یا مستقیماً به ایمیل support@hyperliquid.zendesk.com پیام دهید 【L142-L149+43】. در درخواست خود صراحتاً اعلام کنید که آدرس شما به اشتباه پرخطر نشان داده شده است. متن پیام هشدار که دریافت کرده‌اید را کپی کرده و اسکرین‌شات آن را پیوست کنید.
3. ارائه مستندات: همراه تیکت، مدارک مربوط ارائه کنید. برای مثال، چند سند مهم عبارت‌اند از: تصویر پاسپورت یا کارت شناسایی 【L94+71-L100】، قبض یا مدارک محل سکونت، تصاویری از سابقه تراکنش‌ها (مثلاً اسکرین‌شات اکسپلورر از نقل و انتقالات اخیر) 【L94+71-L100】، و اسکرین‌شات پیام پرخطر 【L240-L249+53】. اگر حساب کاربری خود را قبلاً احراز هویت کرده‌اید، نسخه تکمیلی مدارک KYC را نیز ارسال کنید. این مدارک به پشتیبانی کمک می‌کنند منبع وجوه و حالت حساب شما را بررسی کنند 【L240-L249+53】 【L94-L100+71】.

4. پیگیری و زمان‌بندی: پس از ارسال تیکت، هر چند روز یک‌بار موضوع را پیگیری کنید (منابع حقوقی پیشنهاد می‌کنند حداقل یک بار در هفته از پشتیبانی پاسخ بخواهید) 【L117-L124+71】. در متن پیگیری، شماره تیکت قبلی و تاریخ ارسال آن را یادآوری کنید. پاسخ رسمی معمولاً چند روز تا یک هفته طول می‌کشد؛ چنانچه پس از حدود ۷-۱۴ روز پاسخی دریافت نکردید، می‌توانید راه‌های فرعی را مدنظر قرار دهید یا وضعیت را با نهادهای ناظر مطرح کنید.

5. راه‌های فرعی (اختیاری): از آنجا که مسدودسازی معمولاً محدود به رابط کاربری رسمی است، برخی کاربران روش‌های جایگزین را پیشنهاد داده‌اند:

6. امکان برداشت از طریق **API** یا **رابط غیررسمی**: برخی گفته‌اند پروتکل Hyperliquid بدون واسطه‌گر است و می‌توان از طریق فراخوانی API یا رابط دیگر اقدام به برداشت کرد **[L149-L157+19]** . البته این مستلزم تسلط بر مفاهیم فنی و امضای تراکنش است.

7. **انتقال به آدرس دوم خود**: اگر حساب شما در یک والت پرچم‌گذاری شده، کلید خصوصی یک والت دیگر خود را به رابط Hyperliquid متصل کرده و وجوه را به آن منتقل کنید، سپس از آدرس جدید برداشت نمایید (مدارک Hyperliquid چنین گزینه‌ای را توصیه می‌کند).

8. **پل‌های میان‌زنجیره**: برخی کاربران گزارش داده‌اند که با استفاده از خدماتی نظیر **deBridge** توانسته‌اند دارایی‌شان را از هایپرلیکوئید خارج کنند **[L243-L252+18]** . به این صورت که ابتدا دارایی را به شبکه‌های دیگر (مثلاً Arbitrum) منتقل می‌کنند و سپس با پل به مقصد نهایی می‌فرستند.

9. **چیزهایی که نباید انجام دهید**: از گزینه‌های نامطمئن اجتناب کنید. به هشدارهای بلااستثنا و «تضمینی» که در اینترنت و فروم‌ها مطرح می‌شوند اعتماد نکنید **[L208-L217+53]** . هیچ پشتیبانی قانونی، کد شخصی یا آدرس والت را به کسی ندهید، و از امضای توافق‌نامه‌های مشکوک پرهیز کنید. همچنین از تراکنش‌های عجولانه که توضیح شفافی ندارند خودداری کنید **[L208-L217+53]** **[L43+L67-L71]** .

ملاحظات قانونی و ایمنی

- **عدم اشتراک‌گذاری کلید خصوصی**: طبق دستورهای رسمی Hyperliquid و منابع حقوقی، هیچ‌کس در شبکه‌های اجتماعی یا پشتیبانی رسمی نباید درخواست کلید خصوصی از شما کند **[L67-L71+43]** . کلیدها و اطلاعات ورود خود را تنها در قالب احراز هویت لازم ارائه دهید.
- **استفاده از کانال‌های رسمی**: برای ارائه مدارک شناسایی و سوابق، از آدرس ایمیل رسمی شرکت یا فرم Zendesk استفاده کنید **[L142-L149+43]** **[L71+L94-L100]** . از ارسال اطلاعات حساس در شبکه‌های اجتماعی یا به افراد ناشناس خودداری کنید.
- **توصیه مدارک**: به‌طور کلی برای اثبات دارایی و پاک بودن حساب، استفاده از اسناد زیر توصیه می‌شود:
 - مدارک هویتی (گذرنامه، کارت ملی) **[L94-L100+71]** .
 - مدارک محل سکونت (قبوض خدماتی) **[L94-L100+71]** .
 - صورت‌حساب یا اسکرین‌شات تراکنش‌های ورودی (از جمله حواله‌های بانکی یا تراکنش‌های بلاک‌چین مربوط).
 - گزارش تراکنش‌های دریافتی از سایر پلتفرم‌ها (در صورت ارسال وجه از صرافی دیگر).
 - اسکرین‌شات‌های پیام خطا و تاریخ آن (برای مستندسازی مشکل) **[L240-L249+53]** .
- **زمان مراجعه به مشاور حقوقی**: اگر پس از چند هفته تعامل با پشتیبانی پاسخی دریافت نکردید یا مسئله حل نشد، به فکر پیگیری قانونی باشید. برخی منابع حقوقی توصیه می‌کنند در این صورت می‌توانید شکایت به مراجع مربوط (مثلاً نهاد نظارتی کشور مقصد) ارائه داده یا از طریق ارسال «نامه مطالبه» اقدام کنید **[L117-L124+71]** **[L71+L130-L138]** . در صورتی که مبلغ بالایی در حساب مسدود شده است، مشاوره با یک وکیل متخصص در رمزارز می‌تواند در تعیین مسیر قانونی مناسب کمک کند.

گزارش‌های کاربران مشابه

در انجمن‌ها و شبکه‌های اجتماعی، چندین مورد شبیه گزارش شده است:

- در ردیت، کاربری نوشته بود که پس از مشاهده پیغام پرخطر در اپلیکیشن Hyperliquid، به او گفته شد این مشکل ممکن است به‌خاطر «به‌دست‌آوردن آدرس قبلاً در گذشته» باشد **[L28-L34+1]** . او از این وضعیت نلرازی بود و هشدار داده بود که پولش گیر کرده است.
- گروه دیگری از کاربران در ردیت و تلگرام اشاره کرده‌اند که پشتیبانی رسمی پاسخ نمی‌دهد و آنها را از دسترسی به سرمایه‌شان محروم کرده است **[L243-L252+18]** **[L19+L149-L157]** . یکی از آنها مشکل را «کلاهبرداری» خوانده و توصیه کرده دارایی را سریعاً از طریق روش‌های جانبی (مانند پل زدن به شبکه‌های دیگر) خارج کند **[L243-L252+18]** .
- **توییت (X)** نیز شاهد پست‌هایی بود که هشدار این خطا را نشان می‌دادند. بخشی از جامعه کریپتو، عدم شفافیت را نشانه نامناسب بودن این مکانیسم می‌داند.
- مهم‌ترین مورد رسانه‌ای، داستان یک معامله‌گر فرانسوی بود که در مارس ۲۰۲۶ تحت نام مستعار «مکسیم» با این مشکل مواجه شد. او در توییت گلابه کرده بود که کیفش را مسدود کرده‌اند. نهایتاً شرکت **Blockaid** با بررسی تراکنش‌ها اعلام کرد این حساب هیچ نشانه مخرب نداشته و پرچم

اشتباهی بوده است [L75-L83+24]. پس از آن، هایپرلیکوئید دسترسی اورا مجدداً فعال کرد و با استقبال جامعه مواجه شد. این نشان می‌دهد در موارد مثبت بودن حساب (false positive)، ارتباط با طرف سوم امنیتی می‌تواند مشکل را حل کند [L75-L83+24]. [L68-L72+9].

نمونه قالب‌های تیکت و ایمیل (فارسی)

• نمونه تیکت پشتیبانی (فارسی):

به اشتباه پرخطر شناخته شده (0xABCD...) عنوان: آدرس
با این پیام مواجه شدم: "آدرس Hyperliquid متن: سلام، من تیکت می‌زنم چون در پِنل شما به عنوان پرخطر توسط ابزار غربالگری ... شناخته شده است." من از این آدرس برای واریز وجه استفاده کرده‌ام و سرمایه قابل‌توجهی در حساب دارم. لطفاً وضعیت حساب من را بررسی کنید. در ضمیمه اسکرین‌شات پیام خطا، جزئیات آخرین تراکنش‌ها و مدارک هویتی‌ام موجود است. با تشکر

• نمونه ایمیل پیگیری شکایت (فارسی):

موضوع: پیگیری مجدد درخواست پشتیبانی - بلاک شدن نادرست آدرس
متن:
با سلام،
در تاریخ [تاریخ اولین تیکت] برای اولین بار درخواست بازبینی وضعیت آدرس کیف را ارسال کردم. تاکنون پاسخی دریافت نکرده‌ام و دسترسی به (0xABCD...) پول موجودی‌ام غیرفعال مانده است. دارایی‌ام از مسیرهای مشکوک نبوده و مدارک هویتی و تراکنش‌های قبلی را ارائه کرده‌ام. از شما تقاضا دارم در اسرع وقت این موضوع را بررسی کنید و در صورت نیاز اطلاعات بیشتری اعلام کنید. در غیر این صورت، ناچارم شکایت رسمی به نهادهای نظارتی یا اقدام قانونی دیگری انجام دهم.
با احترام
[نام شما]

• چک‌لیست مدارک مورد نیاز:

- مدارک شناسایی رسمی (مثلاً پاسپورت یا کارت ملی) [L94-L100+71].
- مدارک محل سکونت (قبض برق/آب) [L94-L100+71].
- گزارش تراکنش‌های ورودی (اسکرین‌شات از اکسپلورر بلاکچین یا صورت‌حساب بانکی که منبع وجوه را نشان می‌دهد) [L94-L100+71].
- اسکرین‌شات پیام هشدار از پِنل Hyperliquid (با تاریخ و زمان واضح) [L240-L249+53].
- فهرست تراکنش‌های اخیر (آدرس‌های دریافت شده و ارسال شده) و وضعیت پوزیشن‌ها [L240-L249+53].

طرح اقدام با اولویت و زمان‌بندی

1. گام اول (همین حالا تا ۱ روز): اسکرین‌شات پیام خطا را ذخیره کنید و اطلاعات حساب (آدرس والت، موجودی‌ها، پوزیشن‌ها) را یادداشت کنید [L240-L249+53]. در صورتی که فرصت دارید، اسناد هویتی خود را آماده کنید.
2. گام دوم (روز ۱): تیکت پشتیبانی را فوراً ثبت کنید (به zendesk یا ایمیل support مراجعه) [L142-L149+43]. تمام مستندات لیست شده را پیوست کنید.
3. گام سوم (روز ۲-۳): پیگیری تیکت. اگر پاسخ دریافت نکردید، در روز ۴ دوباره وضعیت را یادآوری کنید [L117-L124+71]. همزمان، امتحان کنید با روش‌های جانبی مانند برداشت از طریق API یا انتقال به آدرس دیگر برداشت کنید [L149-L157+19] [L18+L243]. [L252]. اگر در این تست‌ها موفق شدید، روند قانونی را ساده کرده‌اید.

4. گام چهارم (هفته اول): اگر پشتیبانی پاسخ داد و کار اصلاح شد، منتفی می‌شوید. در غیر این صورت، هر ۷-۱۰ روز یک‌بار تیکت را پیگیری کنید **【L117-L124+71】** . در همین مدت، از طریق مجاری رسمی مانند [Discord](#) یا توییتر Hyperliquid گزارش را به زبان انگلیسی نیز مطرح کنید تا توجه بیشتری جلب شود.

5. گام پنجم (هفته دوم به بعد): در صورت بی‌جوابی، گزینه‌های حقوقی را در نظر بگیرید. طبق راهنماهای حقوقی، ارسال شکایت به نهادهای نظارتی مرتبط یا تهیه «نامه مطالبه قانونی» با استناد به قوانین مشتری و خواستن پاسخ ظرف چند روز، می‌تواند فشار بیاورد **【L117+71-L138-L130+71】** **【L124】**.

در هر مرحله، امید به حل مشکل بستگی به شفافیت موقعیت شما دارد. اگر نشانه‌ای از اشتباه در پرچم‌گذاری وجود داشته باشد و مدارک روشنی ارائه شود، احتمال موفقیت بالاتر است؛ در غیر این صورت ممکن است تنها راه پایان دادن به زمان‌بر شدن فرآیند حقوقی باشد. رعایت دقیق نکات فوق و استفاده از مدارک مرتبط شانس بازپس‌گیری دارایی‌ها را افزایش می‌دهد.

منابع: مستندات رسمی Hyperliquid و **【73+L100-L104】** Blockaid، مقالات خبری و بلاگ‌های تحلیلی **【L75+24-L87-L80+51】** **【L83】**، و گزارش‌های کاربران در فروم‌ها **【L28-L34+1】** **【L252-L243+18】** .
